PRIVILEGE MANAGER
AVAILABLE FOR WINDOWS AND MAC

CONTROL APPLICATIONS AND PRIVILEGES ON ENDPOINTS

PRIVILEGE MANAGER

Provides several application and privilege control implementations

- Whitelisting
- Blacklisting
- Graylisting
- Least Privilege Policy
- Application Privilege Elevation
- Sandboxing / Isolation
- Contextual Application Policies
- Endpoint Grouping
- Monitoring and Logging
- Discovery and Reporting

The flexibility you need to satisfy any number of security requirements:

Privilege Manager operates on a simple 3 step process:

Identify an Application

Evaluate a Policy in Context

Apply an Action

Managing Privileges on Workstations and Servers

Rapidly deploy privilege management on your most sensitive systems and reduce the risk of cyber attacks by controlling if and how applications execute.

OVERVIEW

Privilege Manager, an extension to Secret Server, gives you the ability to better control applications and their privileges on your endpoints. This agent based deployment can help you detect, inventory, monitor, control, and elevate applications on your endpoints based on the rules you put in place.

EASING THE BURDEN OF LEAST PRIVILEGE

Moving towards a Least Privilege model by removing administrative rights from every day employees creates a burden on your Helpdesk or IT Team. Privilege Manager can help alleviate that by allowing you to quickly create policies that empower employees to continue operating as normal, without requiring administrative rights.

INSTALLING APPROVED SOFTWARE

Application Whitelisting, Blacklisting, and Graylisting are the foundation of ensuring that only approved software and processes are allowed to run on your network. Quickly setup policies to allow standard users to install and upgrade approved software.

ADDING PRINTERS AND CHANGING SYSTEM SETTINGS

When locking down your environment, there is a thing as "Too Much" - employees should not have to jump through hoops to add an approved printer or change their system clock. Set policies ahead of time to allow employees to perform the actions they need without requiring administrative rights.

BYPASSING UAC

Many applications require administrative privileges in order to run. With a simple policy in Privilege Manager, you can allow a standard user to run an application without requiring administrative credentials.

PREVENTING MALICIOUS EXECUTIONS

With application blacklists, privilege reduction, and child process execution control you can limit the execution of malicious processes that your antivirus/malware solution may have missed.

Leverage the power of Privilege Manager and Secret Server Together

Making the Crucial Move Towards Least Privilege Easy

According to Microsoft, **over 60% of vulnerabilities in Microsoft Security bulletins were mitigated by running with reduced user rights**. The impact was even greater for Mozilla and Adobe. Malicious software often exploits software vulnerabilities and takes advantage of the rights of the logged in user to infiltrate the computer.

Thycotic customers leverage Secret Server to discover, remove, and control privileged accounts across their network. Once that control is in place, Privilege Manager is used to give flexibility and resources back to the end-users by allowing them to run the programs they need to do in order to continue doing their job.

By combining both solutions, you can implement a defense in depth approach that stops the two methods that attackers use to gain access to your core network services: compromised endpoints and administrative credentials.

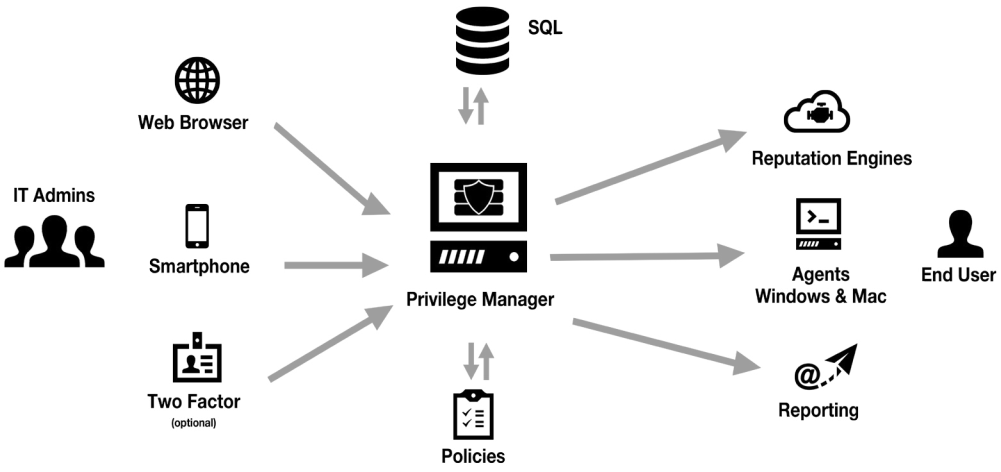
SUPPORTED PLATFORMS

32-bit and 64-bit Windows versions

- Windows XP, Vista, 7, 8, 8.1, 10
- Server 2003, 2008, 2012

Mac Operating Systems

- Mac OS X 10.11



DISCOVER, INVENTORY, AND REPORT

Each agent, installed on your servers, can discover every application and process running on that windows or mac endpoint - so you know exactly what is running on all of your machines. From these inventory reports, you can quickly create policies based on software already used on your network.

Extensive reporting capabilities provide you insight into everything running across your network, while allowing the ability to drill down into individual computer to monitor the activity occurring.

MMC SNAP-IN CONTROL

When you are ready, you can extend the protection of privileges and applications to the rest of your administrative teams. With Privilege Manager, allow your web administrators to access the IIS Web Server and nothing else inside of Microsoft's Management Console (MMC).

ADMINISTRATIVE PERSONAS

Rapidly deploy privileges to your administrator groups with Personas in Privilege Manager. Personas can create roles for your organization (such as the Web Administrator) and define what they are allowed to do on your servers (e.g. Start and Stop the IIS Web Server).

Combined with Active Directory Integration, whenever you assign a new user to that AD group, they will immediately be given the permissions they need to perform their job.

> Privilege Management and application control tools help achieve total cost of ownership (TCO) reasonably close to that of a locked and well-managed user, while giving users some ability to control their systems."

Gartner
"The Cost of Removing Administrative Rights for the Wrong Users" (April 2011)